



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/490,199	01/24/2000	Michael M. Swift	202267	6863

7590 01/04/2005

Leydig Voit & Mayer LTD  
Two Prudential Plaza  
Suite 4900  
180 North Stetson  
Chicago, IL 60601-6780

EXAMINER
----------

ORTIZ, BELIX M

ART UNIT	PAPER NUMBER
----------	--------------

2164

DATE MAILED: 01/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/490,199	SWIFT ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Belix M. Ortiz	2164	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 09/21/2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

  
**SAM RIMELL**  
**PRIMARY EXAMINER**

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

### Remarks

1. In response to communications files on 21-September-2004, claims 1, 6, and 11 are amended per applicant's request. Therefore, claims 1-12 are presently pending in the application.

### *Claim Rejections - 35 USC § 112*

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1-5 and 11-12 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 1 and 11 recite the limitation "accessing, by the proxy client, the target service, the access being in a **batch mode** without user intervention", which is subject matter which was mentioned on the background but not on the summary or on the description of the invention, meaning that is known as a prior art but do not look that batch mode is intended to be used on the invention.

Claims 3, 4, and 5 are rejected under 35 U.S.C. 112, first paragraph, as being dependent from rejected dependent claim 2.

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-2 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gutman et al. (U.S. patent No. 6,298,383) in view of Vu (U.S. patent No. 5,623,601).

As to claim 1, Gutman et al. teaches a method of enabling a proxy client in a secured network to access a target service on behalf of a user (see column 10, lines 47-79), comprising the steps of:

registering proxy authorization information regarding the user with a trusted security server, the proxy authorization information identifying the proxy client and an extent of proxy authorization (see column 1, lines 41-43 and column 10, lines 51-52);

comparing, by the trusted security server, the proxy request with the proxy authorization information of the user to determine whether to grant the proxy request (see column 10, lines 53-55); and

issuing, by the trusted security server, a data structure containing

authentication data recognizable by the target service for authenticating the proxy client for accessing the target service on behalf of the user (see column 1, lines 65-67 and column 9, lines 32-38).

Gutman et al. does not teach submitting, by the proxy client, a proxy request to the trusted security server requesting access to the target service on behalf of the user.

Vu teaches method that provide a security to private and public network (see abstract), in which he teaches submitting, by the proxy client, a proxy request to the trusted security server requesting access to the target service on behalf of the user (see column 5, lines 16-30 and column 8, lines 54-64).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. to include submitting, by the proxy client, a proxy request to the trusted security server requesting access to the target service on behalf of the user.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. by the teaching of Vu, because submitting, by the proxy client, a proxy request to the trusted security server requesting access to the target service on behalf of the user, would enable the method of enabling a proxy client, because "The method in accordance with the invention involves protecting a private network interconnected with a potentially hostile network whereby a gateway between the two networks transparently imitates a host when a communication data packet is received from a client on one of the networks by initiating a communication session with the client. If the client is determined to have access rights to the requested service, the gateway station imitates the client to the host on the other

network by initiating a communications session with the host. Thereafter, data is passed between the client session and the host session by a process which coordinates communications between the two distinct, interdependent communications sessions which proceed between the client and the gateway station and the host and the gateway station”, (see Vu, column 5, lines 15-30).

As to claim 2, Gutman et al. teaches a method wherein the data structure is a ticket containing a session key for use in a session formed between the proxy client and the target service (see Gutman et al., column 2, lines 11-17).

6. Claims 3-8 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gutman et al. (U.S. patent No. 6,298,383) in view of Vu (U.S. patent No. 5,623,601) as applied to claims 1-2 above, and further in view of Higley et al. (U.S. patent No. 5,913,025).

As to claim 3, Gutman et al. as modified still does not teach, wherein the ticket is encrypted with a secret key shared by the target service and the trusted security server.

Higley et al. teaches a method for proxy authentication to access a target (see abstract), in which he teaches wherein the ticket is encrypted with a secret key shared by the target service and the trusted security server (see column 2, lines 18-19).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. as modified, to include wherein the ticket is encrypted with a secret key shared by the target service and the trusted security server.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. as modified, by the teaching of Higley et al., because wherein the ticket is encrypted with a secret key shared by the target service and the trusted security server, would enable the method to maintain the password or key in secret and the client can feel more secure using the network.

As to claim 4, Gutman et al. as modified still does not teach wherein the step of comparing determines whether a proxy duration specified by the proxy authorization information has expired.

Higley et al. teaches a method for proxy authentication (see abstract), in which he teaches wherein the step of comparing determines whether a proxy duration specified by the proxy authorization information has expired (see column 8, lines 16-18).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. as modified to include wherein the step of comparing determines whether a proxy duration specified by the proxy authorization information has expired.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. as modified by the teaching of Higley et al., because wherein the step of comparing determines whether a proxy duration specified by the proxy authorization information has expired, would enable the method to have more control of the access to the network and will be more secure for the clients.

As to claim 5, Gutman et al. as modified still does not teach wherein the step of submitting the request includes transmitting a ticket for authenticating the proxy client to the trusted security server.

Higley et al. teaches a method for proxy authentication (see abstract), in which he teaches wherein the step of submitting the request includes transmitting a ticket for authenticating the proxy client to the trusted security server (see column 5, lines 17-26).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. as modified to include wherein the step of submitting the request includes transmitting a ticket for authenticating the proxy client to the trusted security server.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. as modified by the teaching of Higley et al., because wherein the step of submitting the request includes transmitting a ticket for authenticating the proxy client to the trusted security server, would enable the method to verify the information of the authentication of the client.

As to claim 6, Gutman et al. teaches storing proxy authorization information from a user for authorizing a proxy client to act as a proxy of the user (see column 2, lines 6-10); and

determining, based on the proxy authorization information of the user, whether to grant the proxy request (see column 12, lines 20-24).



Gutman et al. does not teach a computer-readable medium having computer-executable instructions for performing steps:

constructing a data structure containing authentication data recognizable by the target service for authenticating the proxy client for accessing the target service on behalf of the user.

Higley et al. teaches authorization to access a target (see abstract), in which he teaches a computer-readable medium having computer-executable instructions (see column 4, lines 52-58 and column 5, lines 1-2) for performing steps:

constructing a data structure containing authentication data recognizable by the target service for authenticating the proxy client for accessing the target service on behalf of the user (see column 5, lines 17-26).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. to include a computer-readable medium having computer-executable instructions for performing steps:

constructing a data structure containing authentication data recognizable by the target service for authenticating the proxy client for accessing the target service on behalf of the user.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. by the teaching of Higley et al., because a computer-readable medium having computer-executable instructions for performing steps:

constructing a data structure containing authentication data recognizable by the target service for authenticating the proxy client for accessing the target service on behalf of the user, would enable the method to provide a secure network for the clients that want to use the public network.

Gutman et al. as modified still does not teach receiving a proxy request from the proxy client to access a target service on behalf of the user.

Vu teaches method that provide a security to private and public network (see abstract), in which he teaches receiving a proxy request from the proxy client to access a target service on behalf of the user (see column 5, lines 16-30 and column 8, lines 54-64).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. as modified to include receiving a proxy request from the proxy client to access a target service on behalf of the user.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. as modified by the teaching of Vu, because receiving a proxy request from the proxy client to access a target service on behalf of the user, would enable the method of enabling a proxy client, because “The method in accordance with the invention involves protecting a private network interconnected with a potentially hostile network whereby a gateway between the two networks transparently imitates a host when a communication data packet is received from a client on one of the networks by initiating a communication session with the client. If the client is determined to have access rights to the requested service, the gateway station imitates the client to the host on the other network by initiating a communications session with the host. Thereafter, data is passed between the client session and the host session by a process which coordinates communications between the two distinct, interdependent communications sessions which proceed between the client and the gateway station and the host and the gateway station”, (see Vu, column 5, lines 15-30).

As to claim 7, Gutman et al. as modified teaches a computer-readable medium having further computer-executable instructions for performing the step of authenticating the user based on a password of the user before storing the proxy authorization information (see Higley et al., column 5, lines 20-21).

As to claim 8, Gutman et al. as modified teaches a computer-readable medium wherein the step of receiving the proxy request includes authenticating the proxy client based on a ticket issued to the proxy client for communicating with the trusted security server (see Higley et al., column 2, lines 18-19).

As to claim 10, Gutman et al. as modified teaches a computer-readable medium wherein the data structure is encrypted with a key shared by the target service and the trusted security server (see Higley et al., column 2, lines 18-19).

7. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gutman et al. (U.S. patent No. 6,298,383) in view of Vu (U.S. patent No. 5,623,601) and further in view of Higley et al. (U.S. patent No. 5,913,025) as applied to claims 3-8 and 10 above, and still further in view of Subramaniam et al. (U.S. patent No. 6,081,900).

As to claim 9, Gutman et al. as modified still does not teach a computer-readable medium having further computer-executable instructions for performing the step of sending the data structure to the proxy client for presenting to the target service for authentication of the proxy client.

Subramaniam et al. teaches method and system are provided for secure access to a network (see abstract), in which he teaches a computer-readable medium having further computer-executable instructions for performing the step of sending the data structure to the proxy client for presenting to the target service for authentication of the proxy client (see column 15, lines 29-38 and column 16, lines 1-15).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. as modified to include a computer-readable medium having further computer-executable instructions for performing the step of sending the data structure to the proxy client for presenting to the target service for authentication of the proxy client.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Gutman et al. as modified by the teaching of Subramaniam et al., because wherein the security principal is a client on the secured network, would enable the method to be sure that the client has authorization, and that made the network more secure.

8. Claims 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Higley et al. (U.S. patent No. 5,913,025) in view of Gutman et al. (U.S. patent No. 6,298,383) and further in view of Shambroom (U.S. patent No. 6,198,824).

As to claim 11, Higley et al. teaches a computer-readable medium having computer executable instructions for a client in a secured network system (see column 4, lines 50-53) to perform the steps of:

constructing an authenticator encrypted with the session key (see column 2, lines 12-22).

Higley et al. does not teach submitting a proxy request to a trusted security server, the proxy request identifying a user and a target service that the client intends to access on behalf of the user;

receiving from the trusted security server a session key encrypted with a shared secret key shared by the client and the trusted security server and a ticket for accessing the target service; and

decrypting the session key with the shared secret key.

Shambroom teaches a method for enhancing the security on the network (see abstract), in which he teaches submitting a proxy request to a trusted security server, the proxy request identifying a user and a target service that the client intends to access on behalf of the user (see column 5, lines 44-51);

receiving from the trusted security server a session key encrypted with a shared secret key shared by the client and the trusted security server and a ticket for accessing the target service (see column 2, lines 23-32 and 64-67); and

decrypting the session key with the shared secret key (see column 7, lines 46-50 and column 9, lines 16-18).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Higley et al. to include submitting a proxy request to a

trusted security server, the proxy request identifying a user and a target service that the client intends to access on behalf of the user;

receiving from the trusted security server a session key encrypted with a shared secret key shared by the client and the trusted security server and a ticket for accessing the target service; and

decrypting the session key with the shared secret key.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Higley et al. by the teaching of Shambroom, because submitting a proxy request to a trusted security server, the proxy request identifying a user and a target service that the client intends to access on behalf of the user;

receiving from the trusted security server a session key encrypted with a shared secret key shared by the client and the trusted security server and a ticket for accessing the target service; and

decrypting the session key with the shared secret key, would enable the method to know which user is trying to get trough the network and check if he/she have the right authorization to access the network.

Higley et al. as modified still does not teach presenting the authenticator and the ticket to the target service for authentication of the client for access of the target service on behalf of the user.

Gutman et al. teaches the integration of authentication authorization and accounting service and proxy service (see abstract), in which he teaches presenting the authenticator and the

ticket to the target service for authentication of the client for access of the target service on behalf of the user (see column 2, lines 18-25).

Therefore, it would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Higley et al. as modified to include presenting the authenticator and the ticket to the target service for authentication of the client for access of the target service on behalf of the user.

It would have been obvious to a person having ordinary skill in the time the invention was made to have modifies Higley et al. as modified by the teaching of Gutman et al., because presenting the authenticator and the ticket to the target service for authentication of the client for access of the target service on behalf of the user, would enable the method to be more secure for the user because all the information of each user will be protect from others.

As to claim 12, Higley et al. as modified teaches a computer-readable medium wherein the step of submitting the proxy request includes sending a ticket issued to the client for authenticating the client to the trusted security server (see Shambroom, column 5, lines 47-51).

### ***Response to Arguments***

9. Applicant's arguments filed 12- August- 2004 with respect to the rejected claims in view of the cited references have been fully considered but they are not found persuasive:

In response to applicants' arguments that "Ponnekanti, fail to teach or suggest continuing the scan if the row does not satisfy the set of predicates of the query irrespective of current locks", the arguments have been fully considered but are not deemed persuasive,

because Ponnekanti teaches “If, however, the data does not qualify (“no” case), the row is instead skipped, as the row will never qualify” (see Ponnekanti, column 3, lines 62-65).

“If, however, the data does not qualify (“no” case), the row is instead skipped, as the row will never qualify, as indicated by step 322”, (see Ponnekanti, column 15, lines 11-13).

### *Conclusion*

10. Applicant’s amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Belix M. Ortiz whose telephone number is 571-272-4081. The examiner can normally be reached on moday-friday 9am-5pm.

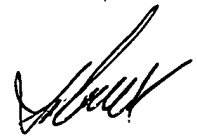


Art Unit: 2164

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on 571-272-4083. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

bmo

December 14, 2004

A handwritten signature in black ink, appearing to read 'S. Rimell', is positioned above the printed name and title.

**SAM RIMELL  
PRIMARY EXAMINER**